(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2001 (19.04.2001)

PCT

(10) International Publication Number
WO 01/28232 A1

(51) International Patent Classification[7]: H04N 5/00, 7/16, 7/167

(21) International Application Number: PCT/US00/27632

(22) International Filing Date: 6 October 2000 (06.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/158,491	8 October 1999 (08.10.1999)	US
60/165,094	12 November 1999 (12.11.1999)	US
60/174,037	30 December 1999 (30.12.1999)	US
09/580,303	26 May 2000 (26.05.2000)	US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: SPRUNK, Eric, J. [US/US]; 6421 Cayenne Lane, Carlsbad, CA 92009 (US).

(74) Agents: FRANKLIN, Thomas, D. et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (US).

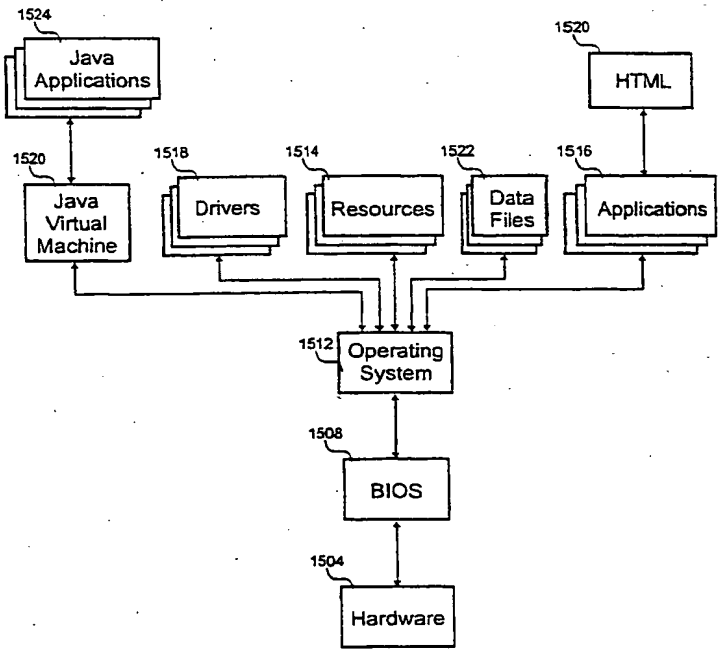
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: OBJECT AND RESOURCE SECURITY SYSTEM



(57) Abstract: Using checkpoints to secure objects and resources in a conditional access system. Authentication and/or authorization checks are performed at a number of checkpoints to assure security of the object and resource. Checkpoints trigger these checks when the purpose of the object or resource becomes manifest as well as other times during handling of the object or resource.

WO 01/28232 A1

OBJECT AND RESOURCE SECURITY SYSTEM

This application claims the benefit of U.S. Provisional Application No. 60/158,491 filed on October 8, 1999, U.S. Provisional Application No. 60/165,094 filed on November 12, 1999 and U.S. Provisional Application No. 60/174,037 filed on December 30, 1999.

BACKGROUND OF THE INVENTION

This invention relates in general to secure access systems and, more specifically, to securing information.

Cable television (TV) providers distribute video streams to subscribers by way of conditional access (CA) systems. CA systems distribute video streams from a headend of the cable TV provider to a set top box associated with a subscriber. The headend includes hardware that receives the video streams and distributes them to the set top boxes within the CA system. Select set top boxes are allowed to decode certain video streams according to entitlement information sent by the cable TV provider to the set top box. In a similar way, other video program providers use satellite dishes to wirelessly distribute video content to set top boxes.

Video programs are broadcast to all set top boxes, but only a subset of those boxes are given access to specific video programs. For example, only those that have ordered a pay per view boxing match are allowed to view it even though every set top box may receive encrypted data stream for the match. Once a user orders the pay per view program, an entitlement message is broadcast in encrypted form to all set top boxes. Only the particular set top box the entitlement message is intended for can decrypt it. Inside the decrypted entitlement message is a key that will decrypt the pay per view program. With that key, the set top box decrypts the pay per view program as it is received in real-time. Some systems sign entitlement messages.

Only recently has storage of multiple hours of video become practical. Each video program is transmitted to set top boxes as a compressed MPEG2 data stream. One hour of video corresponds to about one gigabyte of compressed data. Since multigigabyte storage is common today, multiple hours of video can now be stored. In contrast, conventional CA systems presume content is ephemeral and cannot be stored. In other words, conventional systems are designed presuming that the video programs

In still another embodiment, a method for authenticating and authorizing content supplied to a conditional access set top box is disclosed. Content is received in the conditional access set top box. The content is authenticated a first time within the conditional access set top box. When the content is accessed within the set top box, the content is authenticated a second time.

The invention will be better understood by reference to the following detailed description in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing one embodiment of a content delivery system;

Fig. 2 is a block diagram illustrating an embodiment of a set top box interfaced to its environment;

Fig. 3 is a flow diagram showing an embodiment of a process for distributing an object in a first security level;

Fig. 4 is a flow diagram showing an embodiment of a process for distributing an object in a second security level;

Fig. 5 is a block diagram depicting an embodiment of an authorization message;

Fig. 6 is a block diagram showing an embodiment of an object message;

Fig. 7 is a block diagram illustrating an embodiment of a signatory group that includes portions of the authorization message and the object message;

Fig. 8 is a flow diagram depicting an embodiment of a process for loading an object in a third security level;

Fig. 9 is a flow diagram showing an embodiment of a process for loading an object in a fourth security level;

Fig. 10 is a flow diagram depicting another embodiment of a process for loading an object in the fourth security level;

Fig. 11 is a flow diagram showing an embodiment of a process for checking continuously running objects in a fifth security level;

Fig. 12 is a flow diagram illustrating an embodiment of a process for allowing a free preview of an object in security level six;

Fig. 13 is a flow diagram showing an embodiment of a process for monitoring security checks in security level seven;

unique PID information. There are around one hundred and twenty analog carrier channels in this embodiment of the system 100. Other embodiments could distribute the content with satellite dishes, microwave antennas, RF transmitters, packet switched networks, cellular data modems, carrier current, phone lines, or the Internet.

Referring next to Fig. 2, a block diagram of an embodiment of a display system 200 is shown. This embodiment provides multiple levels of object and resource security through a variety of security levels. Included in the display system 200 are a set top box 108, network 208, printer 212, TV display 216, and wireless input device 218. These items cooperate in such a way that the user can enjoy content provided from a content provider. The content can be video, audio, software, firmware, interactive TV, data, or other information. In this embodiment, the content provider is a cable TV provider.

The network 208 serves as the conduit for information traveling between the set top box 108 and the headend 104 of the cable TV provider. In this embodiment, the network has one hundred and twenty analog channels and a bi-directional control data channel. Generally, the analog channels carry content and the control data channel carries control and entitlement information. Each analog carrier channel has a number of digital channels multiplexed into one data stream where the digital channels are distinguished by packet identifiers (PIDs). The bi-directional control channel is an out-of-band channel that broadcasts data to the set top boxes 108 at one frequency and receives data from the boxes 108 at another frequency. Return data may be queued to decrease overloading during peak use periods using a store and forward methodology well known in the art. Other embodiments could use a cable modem or digital subscriber line (DSL) for both control information and content where the content is formatted as packet switched data.

The printer 212 is an optional accessory some users may purchase and add to their display system 200. When using the set top box 108 for personal computer tasks, the printer 212 allows printing data such as email, web pages, billing information, etc. As will be explained further below, the ability to use a peripheral like a printer is regulated by an authorization check. Using the regulation feature, printers 212 compatible with the set top box 108 do not work unless proper authorization is obtained.

The TV display 216 presents the user with audio and/or video corresponding to the content. The display 216 typically receives an analog video signal that is modulated on a carrier corresponding to channel three, channel four or a composite

This embodiment includes a printer port 232 for interfacing to an optional printer 212. The printer port 232 resource is not available to programs unless authorized. As explained further below, each object must have authorization to use a resource such as the printer port 232. Data is sent from the printer port 232 to the printer 212 in a serial or parallel fashion by way of a wired or wireless transport mechanism.

Stated generally, a checkpoint is a point in time or a step of processing where the authentication and/or authorization status of an object is confirmed. A checkpoint is encountered when printing is requested. The checkpoint authorizes and authenticates the object requesting the printing. Checkpoints are places in one object where authentication and/or authorization are run on another object (e.g., an operating system checks authentication and authorization of an application that is running). Ideally, checkpoints are performed when the purpose of the object becomes manifest. In the case of a printer port 232, its purpose becomes manifest when it is used to print something. Accordingly, a checkpoint is triggered to check the object using the printer port 232 resource when anything is printed. Typically, the checkpoint for printing would be in the operating system.

The network port 236 allows bi-directional communication between the set top box 108 and the headend 104. Included in the network port 236 are a tuner and a demodulator that tune to analog carrier channels and demodulate an MPEG data stream to allow one-way delivery of content. Also included in the network port 236 are a control data transceiver or cable modem that allows for bi-directional communication of control data information and/or content. To distribute loading of the control data path to the headend 104 more evenly, a store and forward methodology may be used.

Modulation of the digital video signal onto an analog signal compatible with the TV display 216 is performed by the display interface 244. As discussed above, the TV display 216 generally accepts signals modulated on channel three, channel four or a composite channel. For displays that accept a digital input, such as LCD displays, the display interface 244 performs any formatting required by the digital input.

The IR port 248 communicates bi-directionally with a wireless input device 218. Included in the IR port 248 is an IR transceiver that provides the wireless communication path with the input device 218. Other electronics in the IR port 248 convert analog signals received by the transceiver to a corresponding digital signal and convert analog signals sent to the transceiver from a corresponding digital signal. The

316. The key is extracted from the entitlement message and used to decrypt the object before it is written to the memory 228 in steps 320, 324 and 328. This process provides both authentication and authorization of the object by using encryption.

Referring next to Fig. 4, a flow diagram of an embodiment of a process for distributing an object in a second security level is shown. In the second level of security, signatures are used to authenticate an object upon download. In other words, the second level of security imposes a checkpoint on the object when downloaded. The signature is generated over a signatory group that includes portions of an authorization message and object message in the headend 104 in step 404. The authorization message is metadata related to the object message and the object message contains the object intended for the set top box 108.

In step 408, the signature in the authorization message and the object are separately sent to the set top box 108 over the network 208. Preferably an asymmetric signature is used (e.g., RSA, DSA or ECC based), but a symmetric signature (e.g., DES or triple-DES) could also be used. Upon receipt of the signature and the object and before storing the object, the signature is calculated and checked by the ACP 240 in steps 420 and 424. If the calculated and received signatures match, the object is stored in step 428. Alternatively, the object is discarded in step 432 if there is no match, and processing loops back to step 412 to wait for another copy of the object.

With reference to Figs. 5-7, an authorization message 500, an object message 600 and a signatory group 700 are respectively shown in block diagram form. Included in the authorization message 500 of Fig. 5 are an authorization header 504, an authorization data structure 508, a signature 512, and a first checksum 516. The authorization message 500 has information used to both authenticate and authorize the object message 600. Forming the object message of Fig. 6 are an object header 604, an object 608 and a second checksum 612. The object message 600 serves as the transport for the object 608. The signatory group 700 includes components of the authorization message 500 and object message 600 arranged end-to-end. The signature 512 is calculated over the whole signatory group 700. More specifically, the signatory group 700 of Fig. 7 includes the authorization header 504, authorization data structure 508, object header 604, and object 608.

The authorization header 504 indicates the configuration of the authorization message 500. Included in the header 504 are a subtype identifier and message version. The subtype identifier distinguishes the various types of authorization

Once the signature is calculated, it is checked against the received signature to authenticate portions of both the authorization and object messages 500, 600. If the signatures do not match, the set top box 108 discards the object message 600 because it presumably came from an improper source.

The first and second checksums 516, 612 are calculated with either linear or non-linear algorithms. These checksums 516, 612 verify the error integrity of the data as it is transported to the set top box 108 over the network 208. For example, the checksum could be a cyclic redundancy check (CRC). The message spooler 208 calculates the checksum 516 as the message 500 is being sent and appends the checksum 516 onto the end of the message 500. Conversely, the set top box 108 calculates the checksum as the message 500 is received and checks the calculated checksum against the checksum 516 in the received message 500. If the calculated and received checksums do not match, an error in transmission has occurred. Messages 500, 600 with errors are discarded whereafter the headend 104 may send replacement messages 500, 600.

The object header 604 includes attributes for the object message 600. Included in the object header 604 are a header length, an object length, the object identifier, the software version, and a domain identifier. The header length and object length respectively indicate the lengths of the object header 604 and the object 608. As described above, the object identifier provides a unique code that allows attributing the authorization message 500 to the object message 600. The software version indicates the version of the object. Different cable TV providers are assigned domain identifiers such that all of the set top boxes 108, which might receive an object 608, can screen for objects 608 associated with their domain.

The object 608 includes content the system 100 is designed to deliver to set top boxes 108. Several types of information can be embedded in an object, such as executable programs, firmware upgrades, run-time programs (e.g., Java® or ActiveX®), programming schedules, billing information, video, audio, or data. The object 608 can be used immediately after authentication and authorization or at a later time. Additionally, authorization can be programmed to expire after a certain amount of time.

Referring specifically to Fig. 7, the signatory group 700 is shown. This group 700 is comprised of parts of both the authorization message 500 and the object message 600. All the data used to calculate the signature 512 is included in the signatory group 700. Because the signature requires components from both the authorization message 500 and the object message 600, a failed signature check indicates one of the

Referring next to Fig. 10, a flow diagram of another embodiment of a process for loading an object in the fourth security level is illustrated. In this embodiment, entitlements in the authorization message 500 are checked in order to confirm the object 608 is authorized before it is loaded. In step 1004, the authorization message 500 is read from the memory 228. Next, the controller 220 loads the authorization message 500 into the ACP 240 in step 1008.

Once the ACP 240 has the authorization message 500, the entitlement information therein is checked in step 1012. A determination is made in step 1016 as to whether the object 608 is authorized by checking the entitlement information. If the object 608 is authorized, it is loaded into memory by the OS and executed. Alternatively, the OS is notified of a failed authorization attempt and object 608 is discarded in step 1024 if there is no entitlement to use the object 608.

Although not express above, the authorization of level four is typically performed coincident with the authentication of level three and before an object 608 is loaded. Authorization is performed prior to authentication because authorization is a quicker process. After the performance of authentication and authorization, the status returned to the OS is NOT AUTHORIZED, AUTHORIZED BUT NOT AUTHENTICATED, or AUTHORIZED AND AUTHENTICATED.

With reference to Fig. 11, a flow diagram of an embodiment of a process for checking continuously running objects in a fifth security level is depicted. As can be appreciated, objects that are running should also be authenticated to be sure they haven't been replaced or modified. Additionally, verifying authorization periodically allows the expiration of an application that has been continuously running for a period of time. A predetermined period can be used or an unpredictably changing period can also be used.

The process begins in step 1104 where the object 608 is read from the memory 228. Before loading the object 608 it has a first signature, but after loading the object 608 into memory 228 the signature of the loaded object is different. As those skilled in the art appreciate, the addresses are translated from virtual addressing to physical addressing such that the signature changes. Accordingly, the signature is recalculated in step 1108 to produce a second signature indicative of the loaded object. It is noted, the object should be loaded and maintained in memory 228 in such a way that the second signature does not change. For example, the loaded object should not have self-modifying code such that the signature would change.

embodiments could use crippled demonstration software that can run forever, but is missing crucial features present in the purchased version. If the user likes the crippled version, the user is likely to purchase the full version to get the missing crucial features.

With reference to Fig. 13, an embodiment of a process for monitoring security checks in security level seven is depicted in flow diagram form. In this embodiment the ACP 240 shadows the OS to double-check that checkpoints are encountered regularly. The process begins in step 1304 where the time of the last OS checkpoint is recorded. Checkpoints are the predetermined places in the OS or other software that cause confirmation of authentication and/or authorization confirmations. Since the ACP 240 is typically involved in the authentication and authorization process, the ACP 240 can track execution of checkpoints. In step 1308, the countdown timer is started. We note once again that this counter could also count-up rather than down.

In step 1312, a determination is made as to whether a checkpoint was observed by the ACP 240. If a checkpoint was observed, processing loops back to step 1304 where the countdown timer is reset so as to start again from the beginning. Alternatively, a check of the timer is performed in step 1316 if no checkpoint is observed. If the counter has not expired, processing loops back to step 1312 to test once again for the observation of a checkpoint. When the timer does expire without reaching a checkpoint, processing continues to step 1320 where the ACP 240 reports an error back to the headend 104.

Although the above embodiment discusses testing for checkpoints on a single object 608, it is to be understood that testing for checkpoints may occur for each object 608 in the set top box 108 in the manner described above. Custom criteria may be designed for each object 608 in order to detect errors in the execution of that object 608. Additionally, we note a trusted or secure operating system normally does not need an ACP 240 to check for aberrant behavior. To thwart hackers, pirates, viruses, and memory errors, checking for normal functioning of the operating system (i.e., check for regular checkpoints) adds an extra layer of security.

Referring next to Fig. 14, a flow diagram of an embodiment of a process for using tokens to achieve an eighth level of security is shown. This embodiment uses a ciphertext token to check authorization of an object 608. The ciphertext token is an encrypted portion of the object crucial to normal operation. Decryption of the ciphertext token produces a plaintext token that is inserted into the object 608 to allow proper execution.

whenever the data in the file is accessed. An HTML object 1528 is reviewed as part of a checkpoint whenever the HTML object 1528 is interpreted by a browser application 1516.

In light of the above description, a number of advantages of the present invention are readily apparent. Having multiple checkpoints that check authorization and/or authentication provides tighter security. With this added security, cable TV pirates are less likely to steal objects, viruses are less likely to go unnoticed and hackers are more likely to be detected.

A number of variations and modifications of the invention can also be used. For example, the above discussion talks of multiple levels of security. It is to be understood that the levels can be combined together to achieve the security goals of a particular system. Additionally, the above embodiments relate to cable TV providers, however, the principals are equally applicable to satellite TV systems, Internet service providers, computer systems, and other providers of content.

The above embodiments discuss several pricing methods for objects. Other embodiments could have one price on the first use and periodically require additional maintenance payments. Further, pricing could be per use with additional amounts per feature. For example, launching the email program is one price and printing each email adds an additional amount. Further still, videos could have a lifetime equal to just less than twice the running time to allow pausing and stopping playback, but not allow viewing the program two times. Video games could have a set lifetime of one hour or one day, for example.

Although the invention is described with reference to specific embodiments thereof, the embodiments are merely illustrative, and not limiting, of the invention, the scope of which is to be determined solely by the appended claims.

7. The method for securing information of claim 6, wherein the step of authenticating the application includes decryption of at least a portion of the information.

8. The method for securing information of claim 1, further comprising steps of:

receiving first authorization information;

receiving second authorization information that replaces the first authorization information so as to extend authorization rights.

9. The method for securing information of claim 1, the method further comprising steps of:

identifying a checkpoint during application execution; and

performing at least one of authentication and authorization in response to the uncovering step.

10. A content delivery system, comprising:

a memory that stores content;

a network port that receives content; and

a plurality of checkpoints in software, wherein each piece of content is subject to at least two checkpoints.

11. The content delivery system of claim 10, wherein each of the plurality of checkpoints initiate at least one of authentication and authorization.

12. The content delivery system of claim 10, wherein the content comprises at least one of: software, drivers, firmware, video, audio, and data.

13. The content delivery system of claim 10, further comprising a content provider coupled to the network port.

14. The content delivery system of claim 10, further comprising an access control processor that performs at least one of the following: authentication and authorization.

authenticating the content a second time when the content is accessed within the conditional access set top box.

22. The method for authenticating and authorizing objects of claim 21, wherein the content comprises one of an object and a resource.

23. The method for authenticating and authorizing objects of claim 21, wherein the conditional access set top box is integrated into an image displaying apparatus.

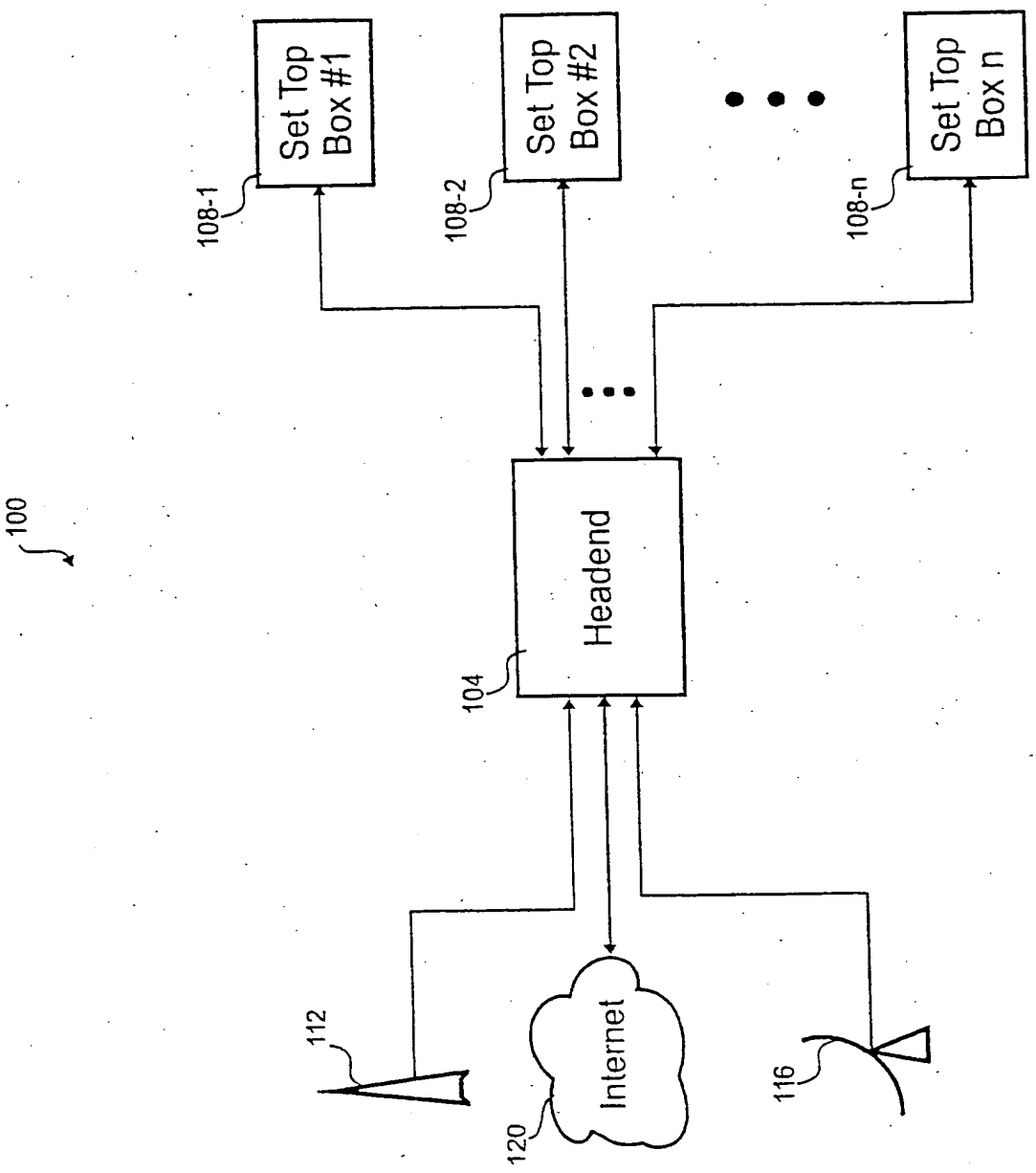

100
Set Top Box #1
108-1
Set Top Box #2
108-2
Set Top Box n
108-n
Headend
104
Internet
120
112
116

Fig. 1

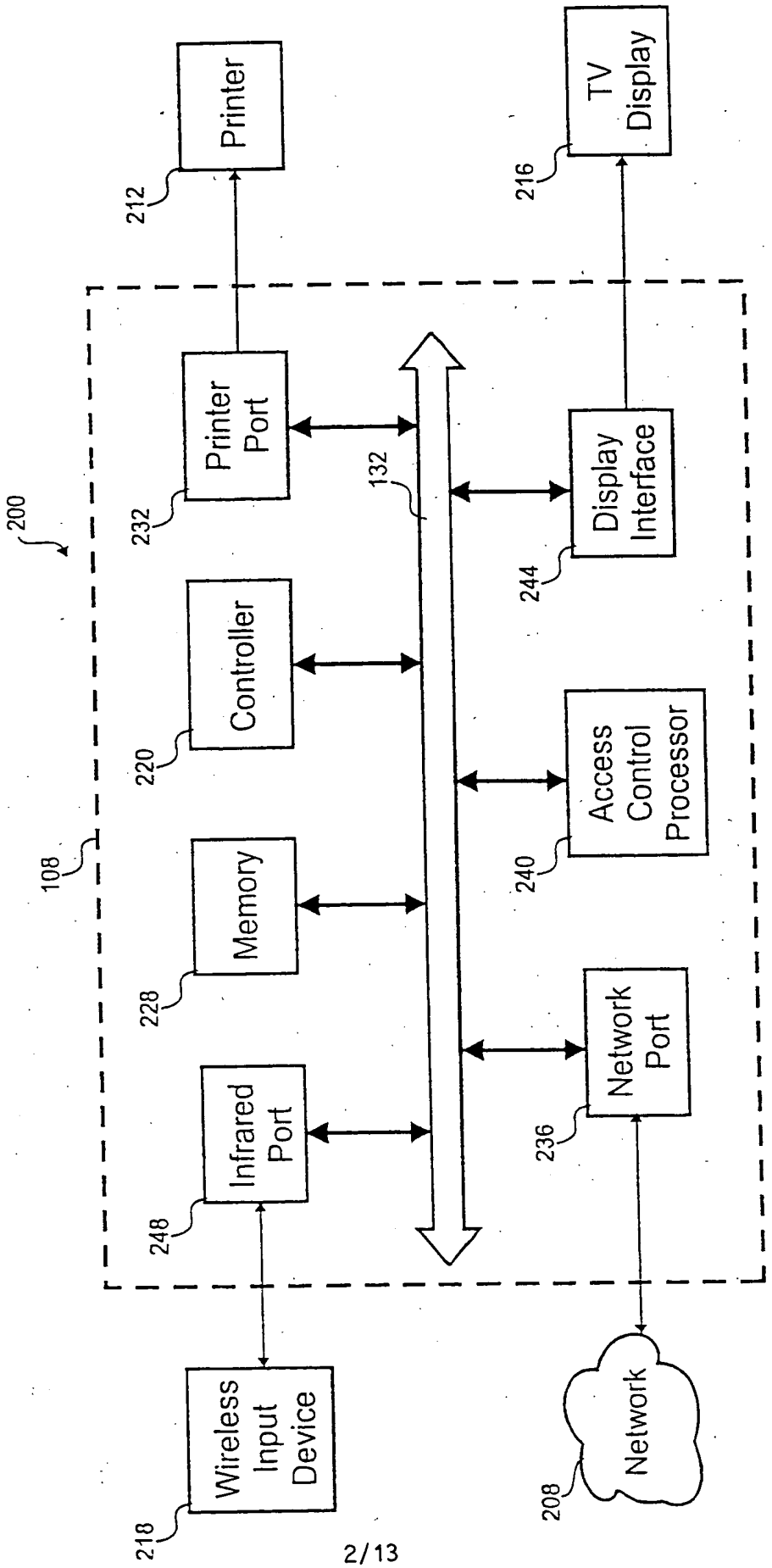

Printer
212
TV Display
216
200
Printer Port
232
132
Display Interface
244
Controller
220
Access Control Processor
240
108
Memory
228
Network Port
236
Infrared Port
248
Wireless Input Device
218
Network
208

Fig. 2

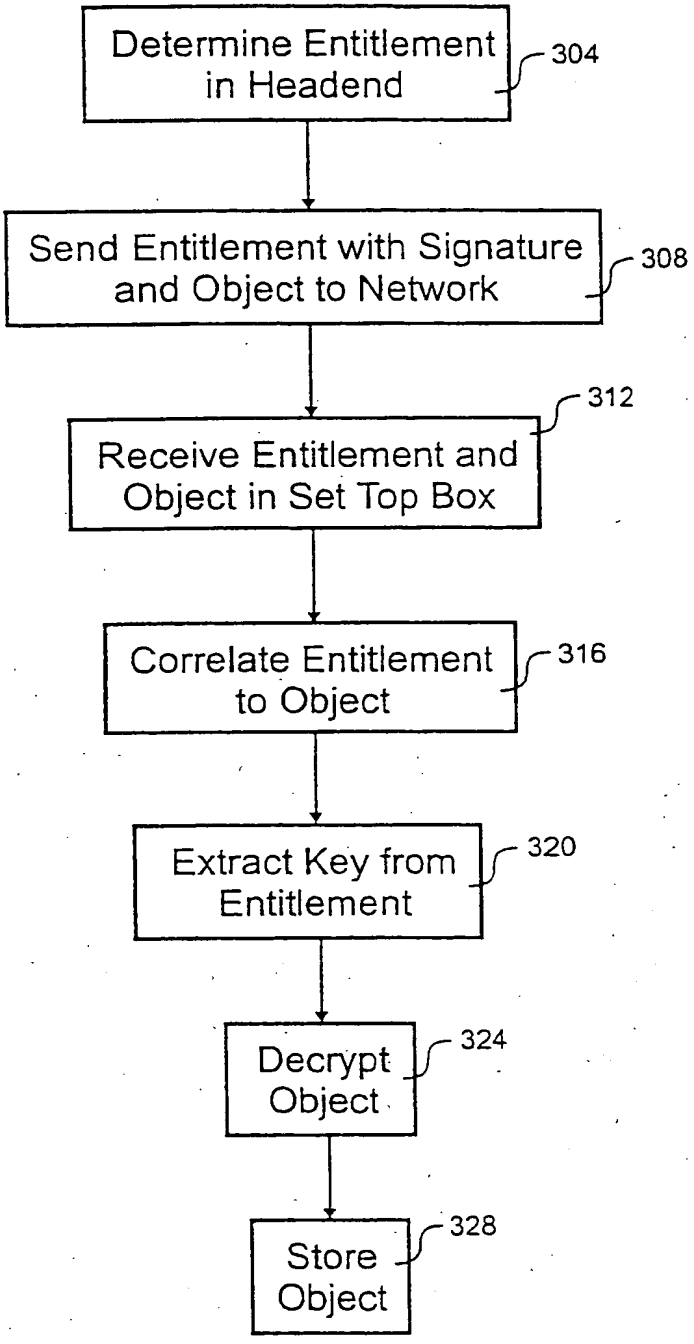

Determine Entitlement in Headend
304
Send Entitlement with Signature and Object to Network
308
Receive Entitlement and Object in Set Top Box
312
Correlate Entitlement to Object
316
Extract Key from Entitlement
320
Decrypt Object
324
Store Object
328

Fig. 3

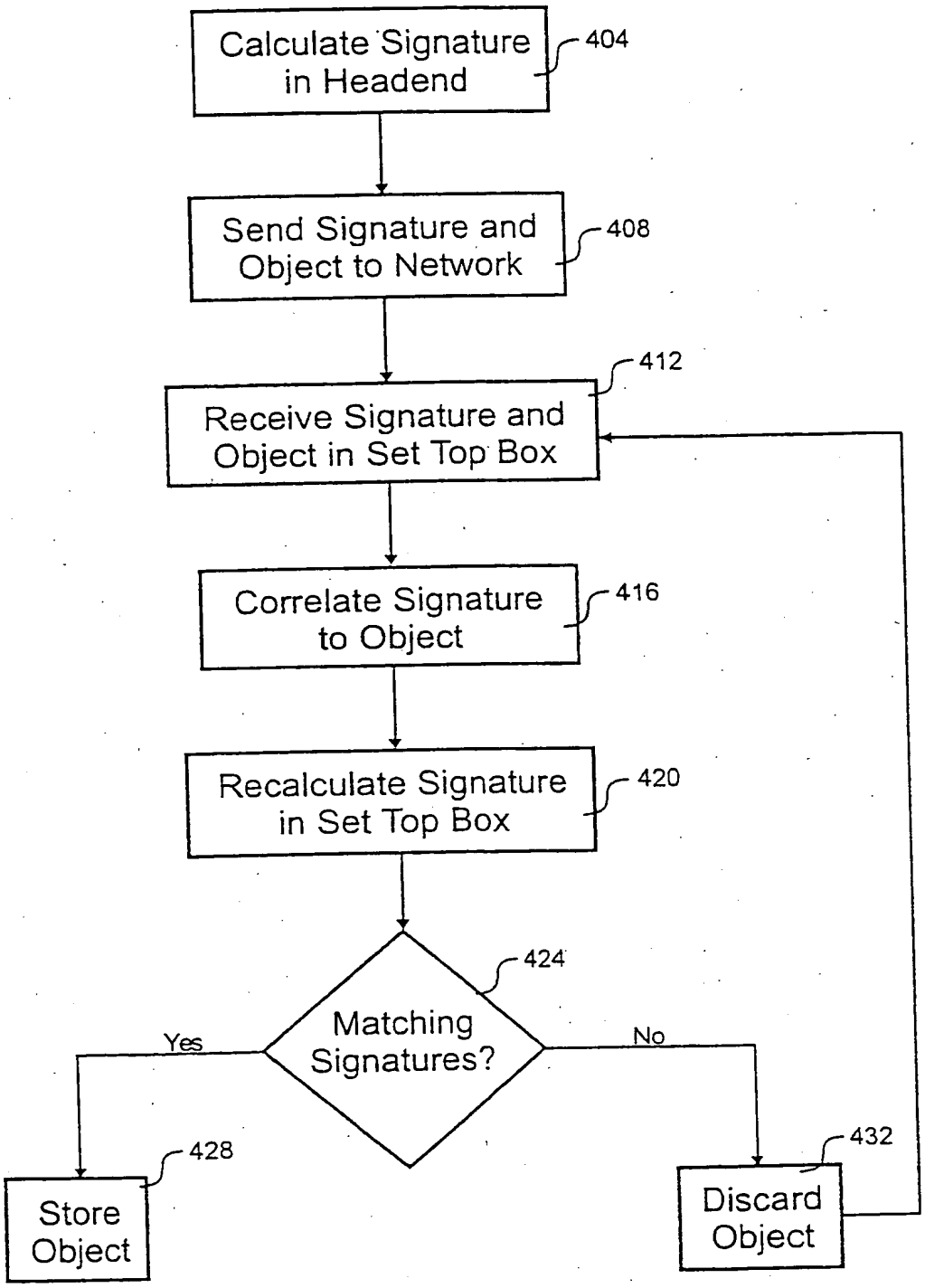

Calculate Signature in Headend
404
Send Signature and Object to Network
408
412
Receive Signature and Object in Set Top Box
Correlate Signature to Object
416
Recalculate Signature in Set Top Box
420
424
Matching Signatures?
Yes
No
428
Store Object
432
Discard Object

Fig. 4

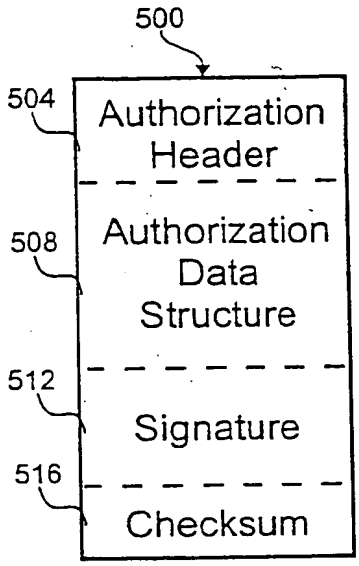


Fig. 5

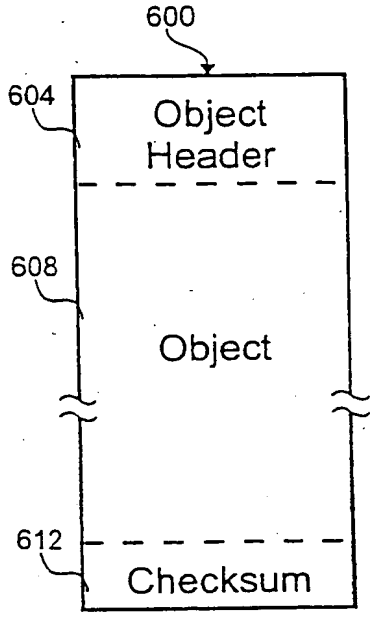


Fig. 6

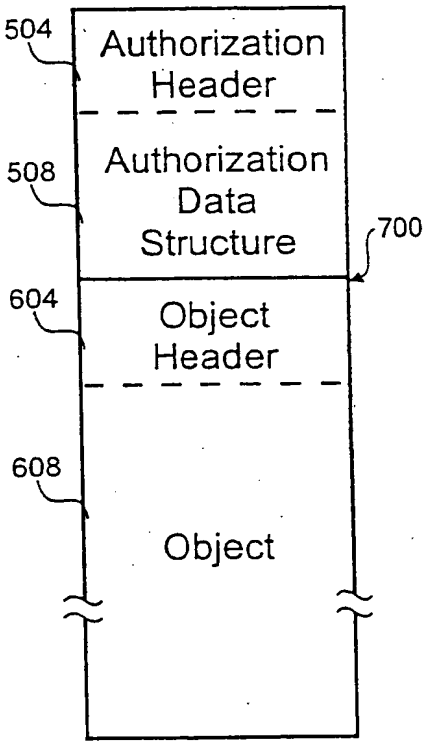


Fig. 7

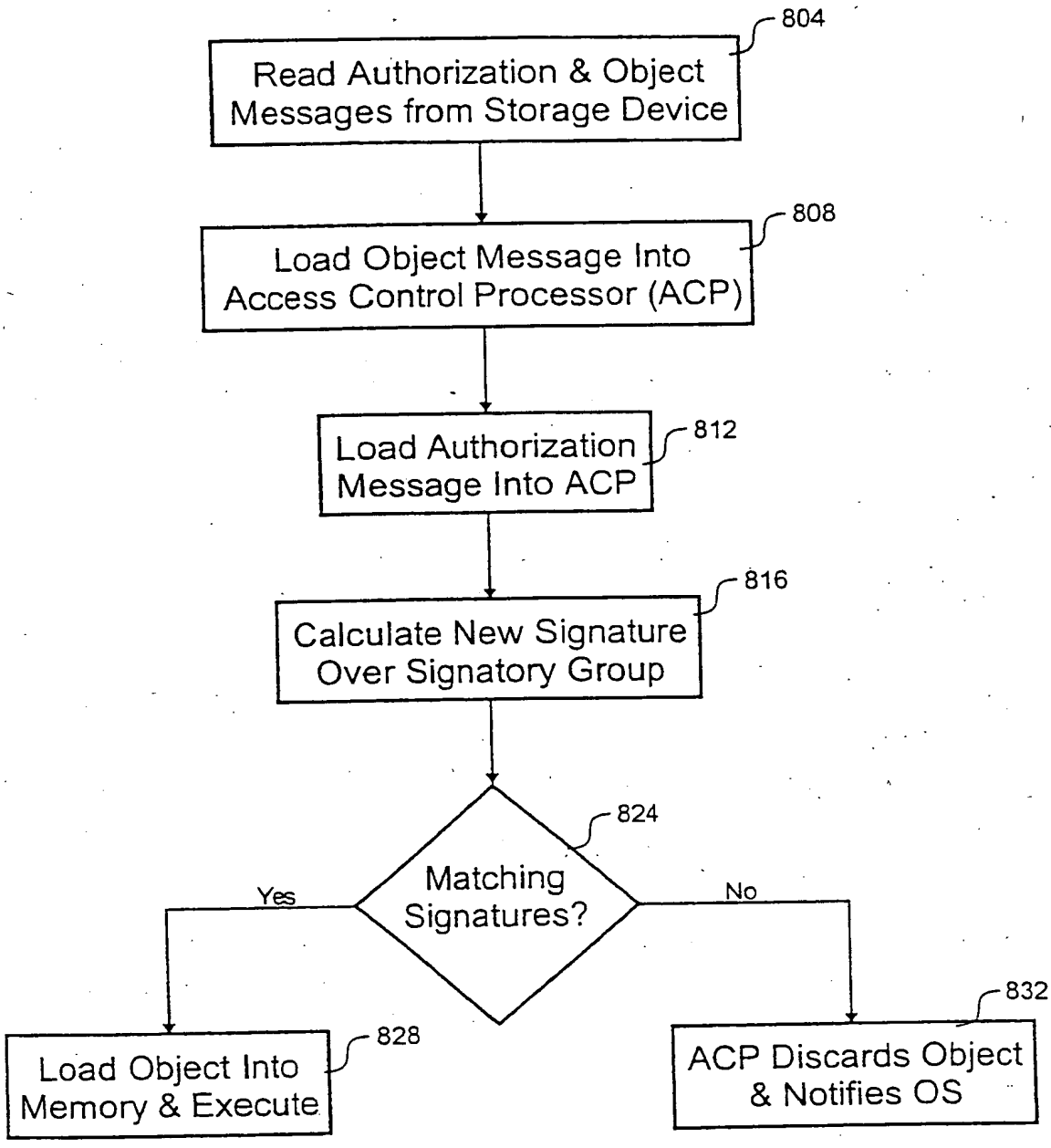

804
Read Authorization & Object Messages from Storage Device
808
Load Object Message Into Access Control Processor (ACP)
812
Load Authorization Message Into ACP
816
Calculate New Signature Over Signatory Group
824
Matching Signatures?
Yes
No
828
Load Object Into Memory & Execute
832
ACP Discards Object & Notifies OS

Fig. 8

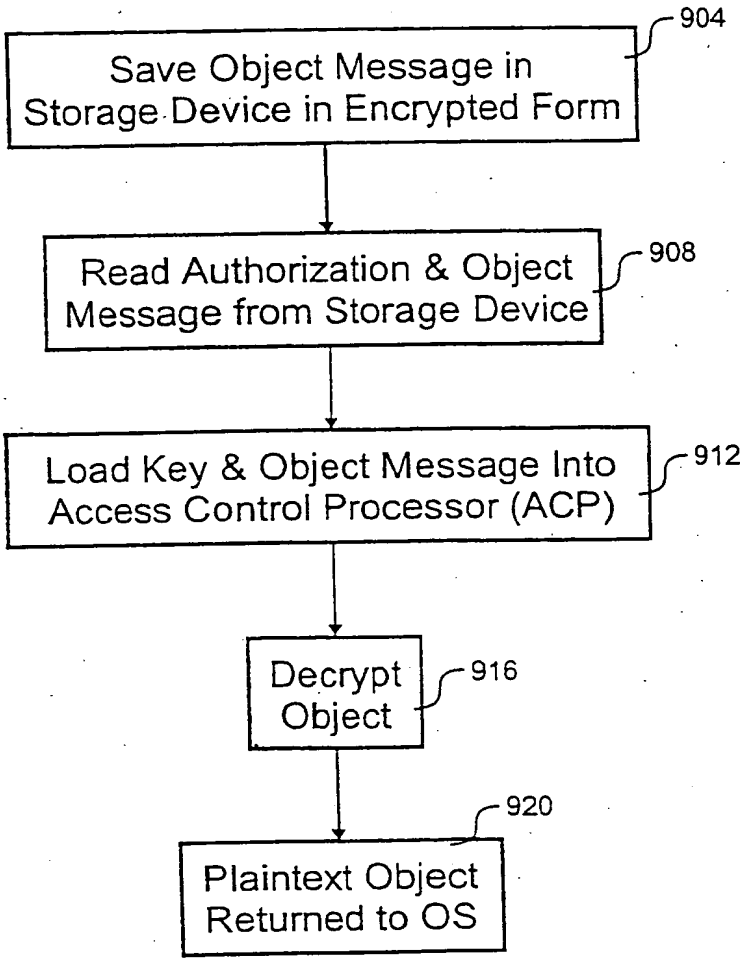

Save Object Message in Storage Device in Encrypted Form
904
Read Authorization & Object Message from Storage Device
908
Load Key & Object Message Into Access Control Processor (ACP)
912
Decrypt Object
916
Plaintext Object Returned to OS
920

Fig. 9

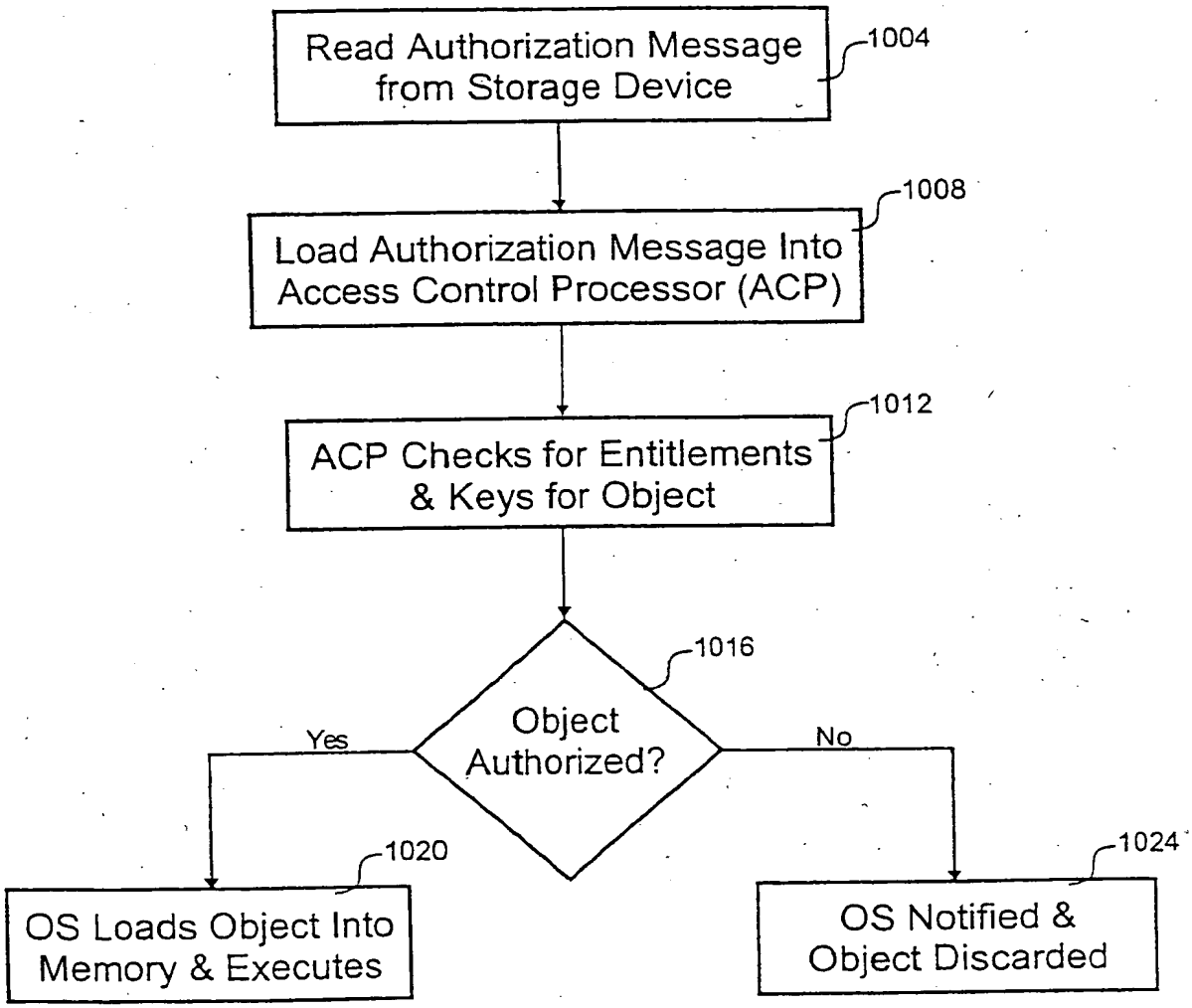

Read Authorization Message from Storage Device
1004
Load Authorization Message Into Access Control Processor (ACP)
1008
ACP Checks for Entitlements & Keys for Object
1012
Object Authorized?
1016
Yes
No
OS Loads Object Into Memory & Executes
1020
OS Notified & Object Discarded
1024

Fig. 10

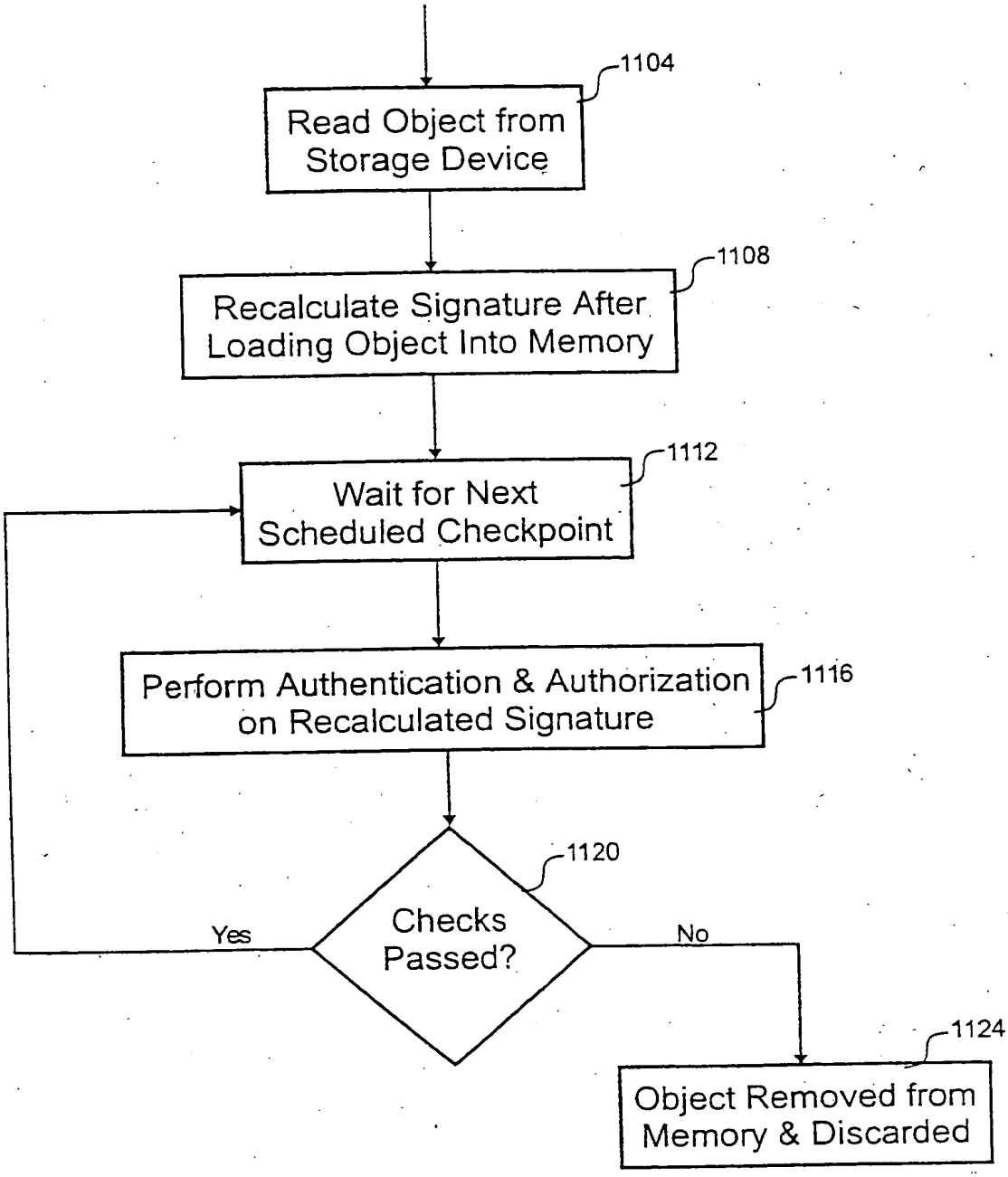

1104
Read Object from Storage Device
1108
Recalculate Signature After Loading Object Into Memory
1112
Wait for Next Scheduled Checkpoint
1116
Perform Authentication & Authorization on Recalculated Signature
1120
Checks Passed?
Yes
No
1124
Object Removed from Memory & Discarded

Fig. 11

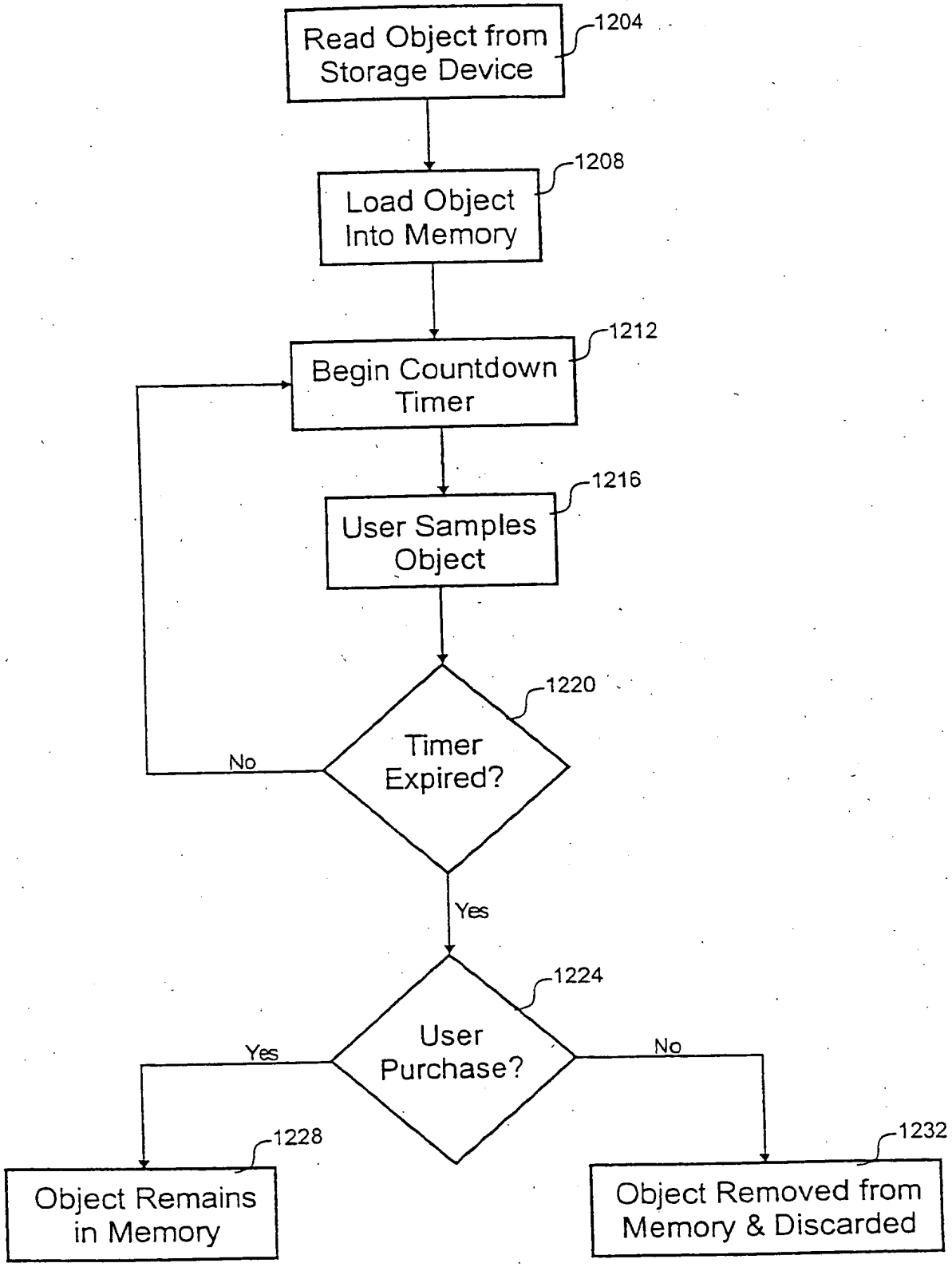

Read Object from Storage Device
1204
Load Object Into Memory
1208
Begin Countdown Timer
1212
User Samples Object
1216
Timer Expired?
1220
No
Yes
User Purchase?
1224
Yes
No
Object Remains in Memory
1228
Object Removed from Memory & Discarded
1232

Fig. 12

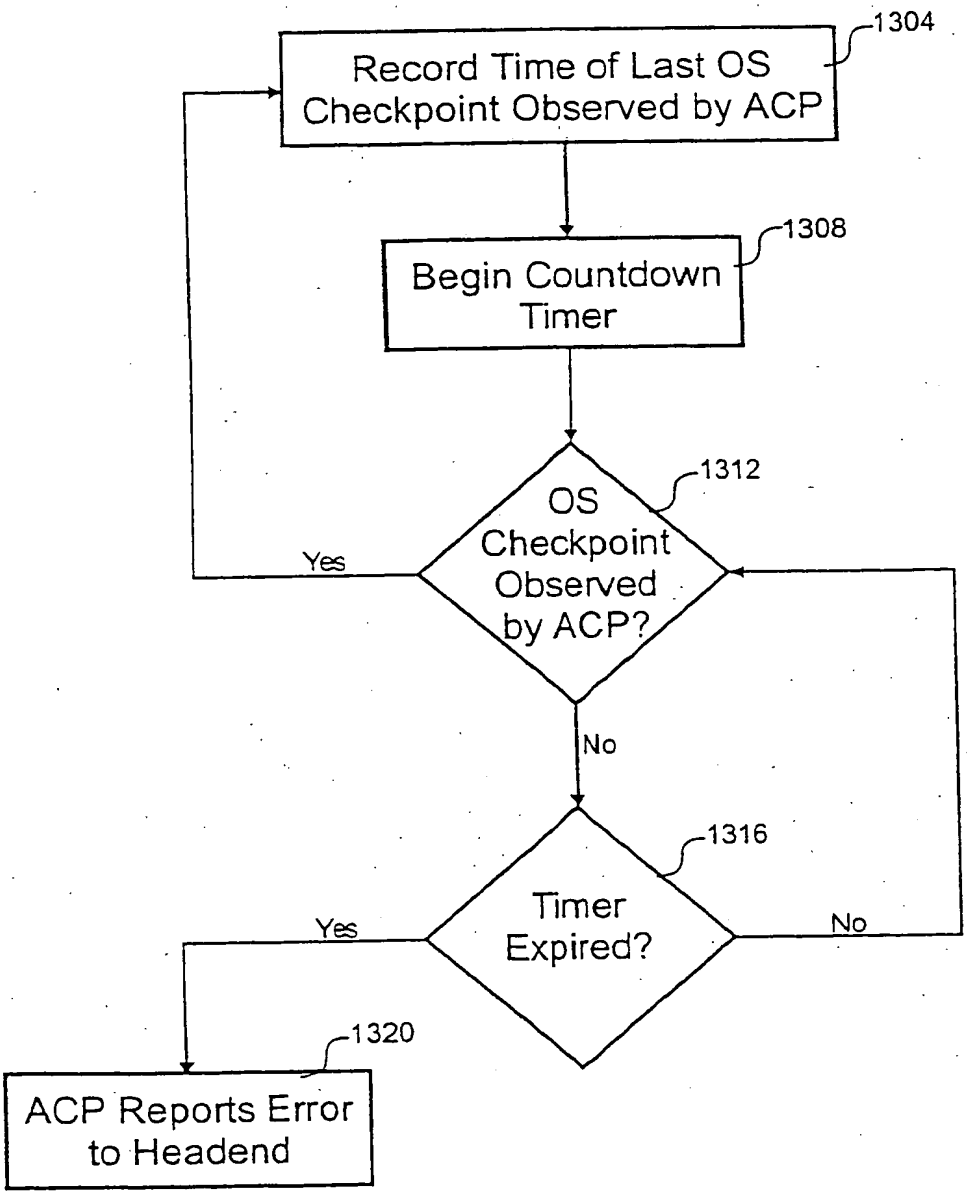

1304
Record Time of Last OS Checkpoint Observed by ACP
1308
Begin Countdown Timer
1312
OS Checkpoint Observed by ACP?
Yes
No
1316
Timer Expired?
Yes
No
1320
ACP Reports Error to Headend

Fig. 13

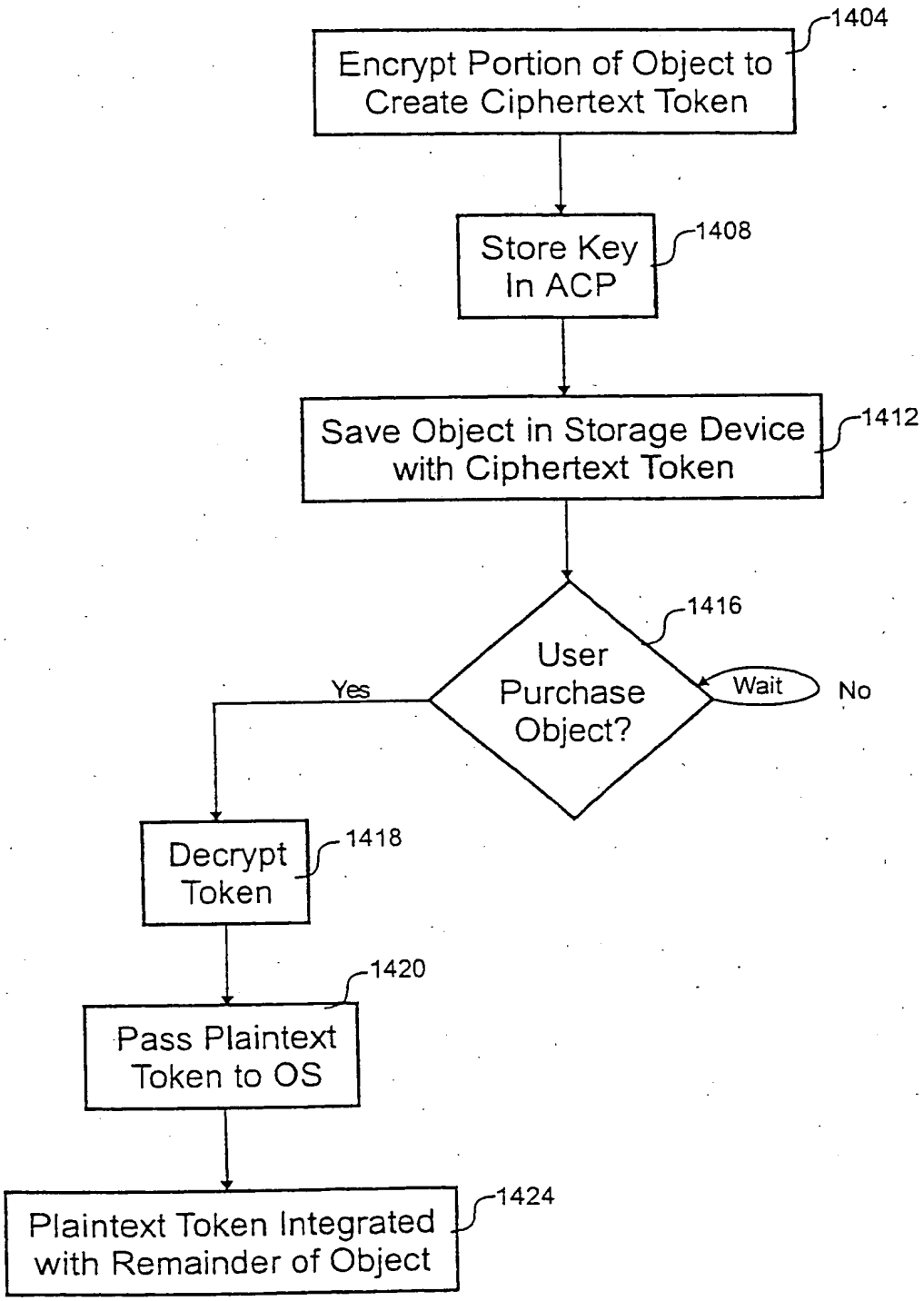

Encrypt Portion of Object to Create Ciphertext Token
1404
Store Key In ACP
1408
Save Object in Storage Device with Ciphertext Token
1412
User Purchase Object?
1416
Yes
Wait
No
Decrypt Token
1418
Pass Plaintext Token to OS
1420
Plaintext Token Integrated with Remainder of Object
1424

Fig. 14

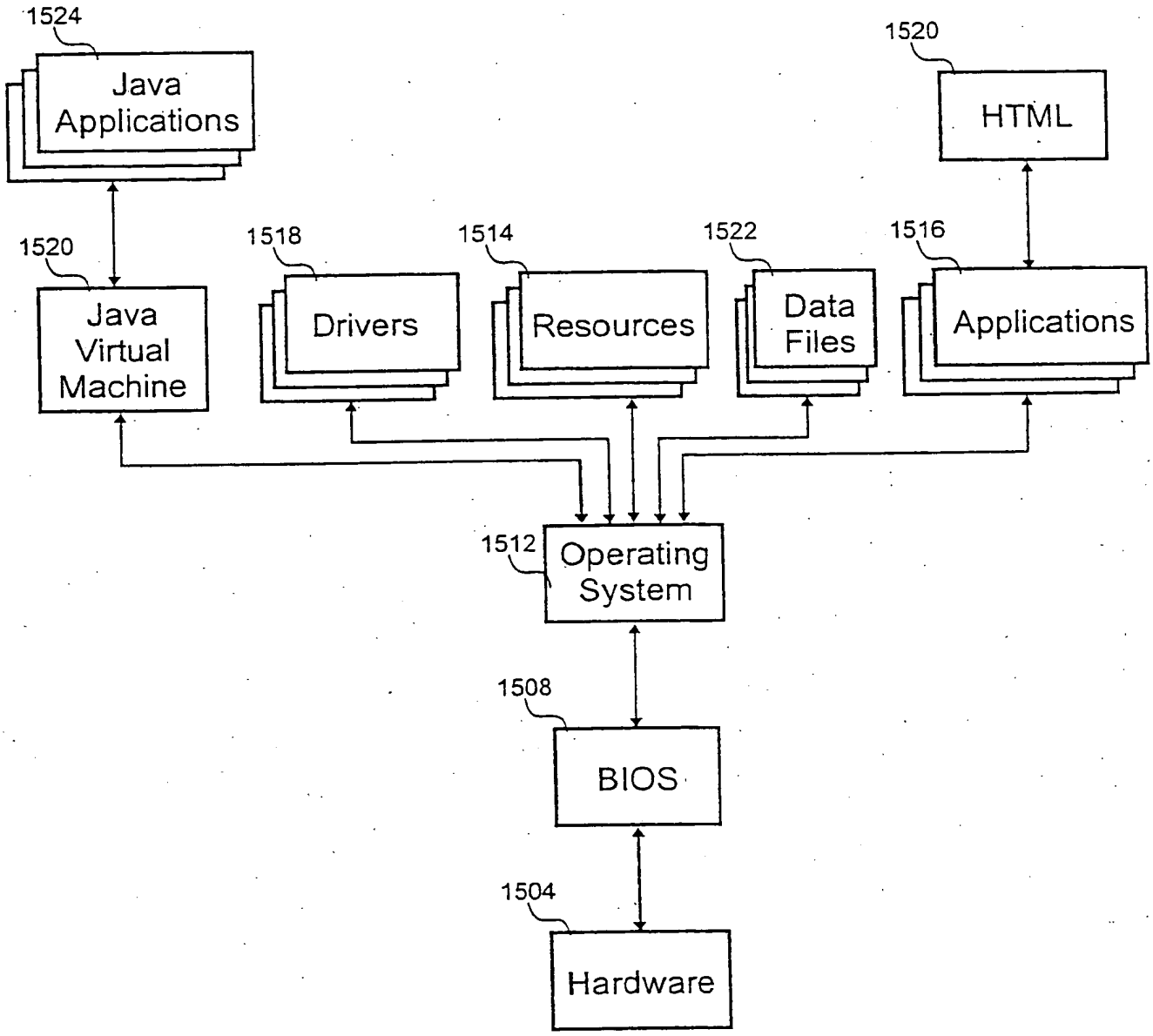

1524
Java Applications
1520
HTML
1520
Java Virtual Machine
1518
Drivers
1514
Resources
1522
Data Files
1516
Applications
1512
Operating System
1508
BIOS
1504
Hardware

Fig. 15

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/US 00/27632

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/00 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 00 04727 A (KONINKL PHILIPS ELECTRONICS NV) 27 January 2000 (2000-01-27)	1,4,5, 10-15, 18,19
P,A	page 4, line 24 -page 5, line 1	21
A	WO 99 39504 A (ACKEN JOHN M ;INTEL CORP (US); SULLIVAN ROBERT R JR (US)) 5 August 1999 (1999-08-05) page 10, line 19 - line 24 page 10, line 28 - line 30 page 11, line 20 - line 23 page 13, line 27 -page 14, line 14 page 16, line 7 - line 11	1,10,15, 21
A	US 5 912 972 A (BARTON JAMES M) 15 June 1999 (1999-06-15) the whole document	1,10,15, 21

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 January 2001	12/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dockhorn, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Inter nal Application No
PCT/US 00/27632

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0004727 A	27-01-2000	BR 9906595 A	18-07-2000
		EP 1048172 A	02-11-2000
WO 9939504 A	05-08-1999	US 6069647 A	30-05-2000
		AU 2216999 A	16-08-1999
		EP 1064788 A	03-01-2001
US 5912972 A	15-06-1999	US 5646997 A	08-07-1997
		US 6115818 A	05-09-2000
		US 6047374 A	04-04-2000
		US 6101604 A	08-08-2000
EP 0946019 A	29-09-1999	AU 2851099 A	18-10-1999
		EP 1064754 A	03-01-2001
		WO 9949614 A	30-09-1999
EP 0752786 A	08-01-1997	US 5625693 A	29-04-1997
		BR 9602980 A	06-01-1998
		CN 1146122 A	26-03-1997
		DE 69606673 D	23-03-2000
		DE 69606673 T	06-07-2000
		ES 2143111 T	01-05-2000
		JP 9121340 A	06-05-1997
		TR 970038 A	21-01-1997